American Journal of Education and Information Technology
2025, Vol. 9, No. 2, pp. 102-110
https://doi.org/10.11648/j.ajeit.20250902.14

Research Article

From Paper Files to Digital Risks: ICT and the Erosion of Confidentiality in South-South Nigerian University Registries

Edho Okugbe Genesis*, Akpotu Nelson Ejiro, Asiyai Romina Ifeoma

Department of Educational Management and Foundations, Delta State University, Abraka, Nigeria

Abstract

Confidentiality has historically defined the professionalism of university registries, serving as the safeguard for records, governance, and institutional trust. In Nigeria, this ethos was once secured by paper-based systems and career administrators. However, the advent of Information and Communication Technology (ICT) has redefined administrative practice, enabled efficiency but also amplified risks. This study investigates how the transition from paper files to digital systems has affected confidentiality in Nigerian university registries. A mixed-methods approach was employed, drawing on survey responses from 596 registry personnel across seven South-South universities, complemented by qualitative interviews. Quantitative analysis revealed that confidentiality is the single strongest determinant of effective administration ($r = .972$, $p < .001$), while ICT competence also demonstrated a significant influence ($r = .801$, $p < .001$). Qualitative findings highlighted breaches unique to the digital era, including unauthorized WhatsApp circulation of Council minutes, covert recordings with smartphones, and tampering with e-records. Comparative analysis showed that while pre-ICT breaches were localized and manual, post-ICT breaches are instantaneous, viral, and systemic. The findings confirm that ICT has transformed confidentiality from a cultural expectation into a measurable competence that must be embedded in training, professional regulation, and data protection frameworks. The study concludes that registry professionalism in the digital era requires enforceable NDPA-aligned policies, ICT-based safeguards, and stronger professional accountability mechanisms.

Keywords

Confidentiality, ICT, Registry Professionalism, Nigerian Universities, Data Protection, Higher Education Administration

1. Introduction

Registry is universally acknowledged as the administrative heartbeat of the university system, a hub where academic and governance machinery intersect. In Nigeria, the Registry has long been entrusted with the custodianship of records, interpretation of university laws, preparation of Council and Senate papers, management of admissions, and authentication of student and staff records [1, 2]. Registrars and their personnel were historically career administrators, carefully nurtured through years of mentoring, rotation, and structured training [3]. This career pathway cultivated professionalism, discretion, and above all, confidentiality, the defining ethos that registry personnel are “seen but not

*Corresponding author: ogedho@delsu.edu.ng (Edho Okugbe Genesis)

Received: 3 September 2025; **Accepted:** 12 September 2025; **Published:** 26 September 2025

heard."

In the pre-ICT era, confidentiality was safeguarded largely by physical controls: restricted access to paper files, hierarchical clearance systems, and reliance on organizational loyalty [4]. Breaches, when they occurred, were slow and localized—manual file concealment, transcript alterations, or selective disclosure of information. However, the 21st century ushered in a digital revolution that has profoundly disrupted these safeguards. Information and Communication Technology (ICT) has transformed how records are created, stored, and transmitted, enhancing efficiency but also multiplying opportunities for breaches. Smartphones, social media, and cloud storage now make sensitive university data transferable in seconds, easily leaked beyond institutional boundaries, and often impossible to retract.

Evidence from [8] confirms the scale of this challenge: confidentiality, once the most reliably practiced professional value, remains the single strongest predictor of effective administration ($r = .972$, $p < .001$), however paradoxically, it is also the weakest in practice. This paradox underscores a deeper institutional problem—while universities adopt ICT systems and cite compliance with the Nigeria Data Protection Act (NDPA, 2023), daily practice often lags, leaving confidentiality exposed to technological vulnerabilities.

The problem is not confined to Nigeria. Globally, higher education is increasingly vulnerable to cyber threats. For instance, the Australian National University was breached in a highly sophisticated attack affecting nearly two decades of data [14]. In the United States, UCSF paid a $1.14 million ransom following a ransomware incident [15, 16]. More recently, the Tshwane University of Technology in South Africa suffered a significant breach that led to the suspension of a senior registrar [11, 12].

This study investigates the following research questions:

1. How has ICT adoption reshaped confidentiality practices in Nigerian university registries?
2. What forms of confidentiality breaches are most prevalent in the digital era compared to the paper-based era?
3. How do confidentiality and ICT competence statistically predict effective university administration?

This article therefore focuses on the erosion of confidentiality in the Registry through the lens of ICT transformation. It examines the historical shift from paper-based safeguards to digital risks, drawing on evidence from seven South-South Nigerian universities and enriched by African and global cases. The paper applies Institutional Theory to explain why universities adopt ICT platforms and data protection frameworks for legitimacy but fail to ensure consistent implementation. By isolating confidentiality and ICT from other best practices, this study offers a sharper evidence-based contribution to understanding how the Registry can reclaim its role as the trusted custodian of university governance in the digital era.

2. Literature Review

2.1. Historical Perspectives on the Nigerian Registry

Confidentiality has long been regarded as the defining ethos of university registry practice. Historically, registries functioned as the custodians of institutional memory, with staff expected to uphold discretion in all administrative processes. The Registrar has been described as a 'custodian of secrets' [1]," entrusted with records, minutes, and sensitive correspondence. This ethic of confidentiality was reinforced by structured career pathways and professional mentoring [3], which nurtured loyalty, discipline, and discretion.

However, the advent of Information and Communication Technology (ICT) has transformed both the possibilities and vulnerabilities of administrative practice. [8] argued that paperless systems promised transparency, efficiency, and speed in Nigerian universities, but warned that without confidentiality safeguards, technology could magnify administrative risks. A global review reached a similar conclusion, noting that digital dual systems (manual and electronic) often introduced inconsistencies, errors, and opportunities for breaches [5].

The Nigerian context reflects these global patterns. Evidence from South-South universities indicates weak infrastructure and records management [6]. Research has demonstrated that staff self-efficacy significantly affects records management, but confidentiality breaches undermine trust in data handling regardless of technical competence [7]. More recently [8] provided empirical evidence that confidentiality is the strongest predictor of effective administration ($r = .972$, $p < .001$), however registry staff rated it as one of the weakest practiced competencies (mean = 2.29). This contradiction underscores the tension between professional ideals and operational realities.

Globally, high-profile cases underscore that confidentiality failures are not unique to Nigeria. The University of Greenwich (UK) was fined £120,000 in 2018 under GDPR after a major student data breach. UCSF paid a ransom following a ransomware incident [15, 16], and the Australian National University published a detailed report on its 2018 data breach [14]. In Africa, the University of Johannesburg mistakenly emailed confidential student records to thousands in 2022, and Tshwane University of Technology fell victim to a ransomware attack in 2023. These cases illustrate how ICT adoption, without corresponding cultural and regulatory reinforcement, exposes universities to reputational and legal risks.

The application of Institutional Theory provides an interpretive framework for these patterns. Universities adopt ICT platforms, confidentiality policies, and compliance mechanisms such as the Nigeria Data Protection Act (NDPA, 2023) under coercive (legal), normative (professional), and mimetic (global) pressures. However, implementation often remains

weak, resulting in what [13] describe as "decoupling": formal structures exist to project legitimacy, but daily practice diverges. In Nigerian universities, this explains why ICT adoption coexists with rampant breaches policies are adopted for legitimacy, but confidentiality culture is neither enforced nor internalized.

Taken together, the literature establishes three critical insights. First, confidentiality remains the keystone of registry professionalism. Second, ICT is a double-edged sword both enabling efficiency and amplifying risks. Third, Nigerian universities illustrate a global paradox: adopting ICT and compliance frameworks for legitimacy but failing to embed confidentiality in practice. This sets the stage for the present study, which empirically explores the erosion of confidentiality in the digital era through comparative pre-ICT and post-ICT breaches.

2.2. Confidentiality as the Core of Professionalism

Confidentiality has historically distinguished the Registry from other administrative units. Registry personnel were entrusted with sensitive materials—admission lists, examination records, Council minutes, and staff files and expected to guard them with discretion. [9] described the Registry as the "heartbeat" of the university, insisting that without confidentiality, institutional credibility collapses.

However, breaches of confidentiality are increasingly reported. [3] documents how unauthorized disclosures of Council decisions, premature announcements of appointments, and the sale of student transcripts have undermined trust. [8] found that while confidentiality showed the strongest statistical correlation with effective administration ($r = .972$, $p < .001$), it was also the weakest practiced domain (mean = 2.29 < 2.50 benchmark). It is an irony that confidentiality, though rhetorically celebrated, is practically neglected.

Globally, confidentiality is recognized as central to higher education administration, where professionalism and discretion remain essential for sustaining institutional trust. [5], studying international registries, emphasized that confidentiality, diligence, and accountability are universal markers of effective registry service. The literature converges on one conclusion: confidentiality is not optional but foundational.

2.3. ICT and Confidentiality: The Double-Edged Sword

Information and Communication Technology (ICT) has transformed registry operations worldwide. From electronic admissions portals to e-senate meetings, ICT enables speed, efficiency, and transparency. [8] advocated for paperless systems as a route to modernisation but cautioned that without confidentiality safeguards, ICT could amplify breaches. [6], focusing on South-South Nigerian universities, reported poor records management and weak ICT infrastructure as drivers of confidentiality lapses. [7] demonstrated that ICT competence and self-efficacy directly influence records management outcomes.

The ethical dilemmas of AI in higher education highlight the need for strict confidentiality protocols to prevent digital innovation from backfiring [10]. South African experience is illustrative: under the Protection of Personal Information Act (POPIA), universities such as Stellenbosch and Tshwane University of Technology faced scrutiny for data breaches, including ransomware attacks (2023). These cases show that ICT both enables efficiency and exposes vulnerabilities.

Globally, the literature is rich with cautionary tales. The University of Greenwich (UK) was fined £120,000 in 2018 for a data breach under GDPR. Medical research was severely disrupted following a ransomware attack [16], while a sophisticated intrusion compromised staff and student records [14]. Together, these cases highlight ICT as a double-edged sword: a tool for efficiency but also a conduit for large-scale confidentiality failures.

2.4. Gen Z Staff and Digital Culture

This generational shift requires more than awareness: institutions must deliberately train and monitor younger staff whose instinctive use of social media normalizes oversharing [19]. Survey evidence revealed that Gen Z personnel were significantly more likely to engage in practices such as screenshotting official documents or forwarding unofficial updates on WhatsApp compared to older colleagues. Such behaviours blur professional and personal boundaries, and unless guided by strong confidentiality codes, they erode trust in registry operations. International studies echo this trend, noting that digital-native employees require targeted professional ethics training to counteract habits of casual disclosure.

An emerging strand of literature considers generational change. Gen Z, born between 1997 and 2012, are digital natives whose social media practices normalize instant sharing. While this generational cohort brings valuable ICT fluency, it also introduces risks. WhatsApp, Instagram, and TikTok cultures blur professional and personal boundaries, leading to oversharing of sensitive information.

Evidence from Nigerian universities reflects this shift. Registry staff increasingly report unauthorized screenshots of confidential documents, audio recordings of meetings, and forwarding of draft bulletins before official release. Globally, similar patterns are evident: Harvard (USA) faced exposure of faculty emails during admissions litigation in 2018, while South African universities have struggled with leaks via student and staff WhatsApp groups [17, 19]. However empirical literature specifically addressing Gen Z in African university administration remains limited, highlighting a research gap that this article seeks to address.

2.5. Policy and Regulatory Frameworks

The regulatory environment is tightening around confidentiality. Nigeria's National Data Protection Act (NDPA, 2023) establishes lawful processing, data minimization, breach notification, and sanctions for non-compliance. The Nigeria Data Protection Commission (NDPC) has reinforced compliance obligations, with directives such as the 2025 General Administrative Implementation Directive (GAID) mandating breach reporting within 72 hours.

Internationally, frameworks such as the EU's General Data Protection Regulation (GDPR), the USA's Family Educational Rights and Privacy Act (FERPA), and South Africa's POPIA underscore the universality of confidentiality obligations in higher education [17]. These frameworks carry reputational and financial penalties, signalling that confidentiality breaches are not only professional lapses but legal violations.

Professional associations also play a role. However, unlike the Institute of Chartered Accountants of Nigeria (ICAN) or the Nursing and Midwifery Council of Nigeria (NMCN), which enforce standards and discipline members, ANUPA and ARNU lack statutory authority. As a result, breaches often go unsanctioned, reinforcing a culture of impunity. [8, 18], argue that unless these associations transform into regulatory bodies with enforcement powers, registry professionalism will remain fragile.

2.6. Summary of the Literature

The literature establishes three consistent insights:

1) Confidentiality is foundational to registry professionalism, historically secured through tradition but now under severe strain.
2) ICT is indispensable however risky, enabling efficiency while multiplying breach opportunities, especially in environments with weak controls.
3) Generational change (Gen Z) introduces new dynamics, as digital culture amplifies confidentiality risks.

What is missing, however, is integrated scholarship that links confidentiality and ICT through empirical Nigerian evidence while accounting for generational shifts and global regulatory frameworks. This article addresses this gap by situating Nigerian experiences within broader African and global debates.

3. Methodology and Findings

This study employed a mixed-methods design to examine the role of confidentiality and ICT in effective university administration. The quantitative component surveyed 596 registry staff drawn from seven universities in Nigeria's South-South geopolitical zone, while the qualitative component included semi-structured interviews with senior administrators. The mixed-methods approach allowed for both statistical measurement of relationships and contextual understanding of confidentiality practices and breaches. The survey respondents (n=596) were selected using a stratified purposive sampling strategy to ensure representation across senior, middle, and junior registry staff. The questionnaire was pre-tested with 20 registry staff for clarity and reliability. Instrument validity was confirmed through expert review, and reliability analysis produced a Cronbach's alpha of 0.87, indicating high internal consistency.

3.1. Quantitative Measures

The instrument captured ten registry best-practice domains identified by [8]. For the purpose of this paper, the analysis narrows to confidentiality and ICT competence, measured on a 4-point scale (1 = Very Low, 4 = Very High). Effective administration was operationalized through measures of governance credibility, trust, and staff morale. Pearson correlation analysis revealed that confidentiality was the strongest and most significant predictor of effective administration.

Table 1. *Correlation Between Confidentiality, ICT, and Effective Administration.*

Variable Pair	Pearson Correlation	Sig. (2-tailed)	N
Confidentiality ↔ Effective Admin	.972**	.000	493
ICT Competence ↔ Effective Admin	.801**	.000	493

Note: $p < .001$. Source: Field survey [8].

These results confirm that confidentiality is the keystone competence, with ICT competence also exerting a strong positive influence. Other practices such as punctuality and regularity, while traditionally celebrated, showed no significant correlation with effectiveness.

3.2. Qualitative Insights

The interviews revealed patterns of confidentiality breaches across both pre-ICT and ICT-driven contexts. Re-

spondents recalled breaches in the paper-based era, such as concealed files, altered transcripts, and selective leaks of sensitive decisions. However, ICT has amplified both the speed and scale of breaches. Commonly cited digital-era practices included:

1) Unauthorized WhatsApp forwarding of Council minutes.
2) Covert smartphone recordings of Senate and Council meetings.
3) Password tampering in e-transcript systems.
4) Unsecured storage of records in personal cloud accounts.

These insights reinforce the statistical findings by showing how ICT, while indispensable for modern administration, has introduced new vulnerabilities.

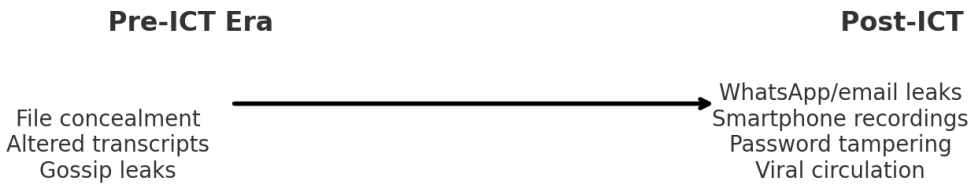
3.3. Comparative Analysis: Pre-ICT vs Post-ICT Breaches

Table 2. Confidentiality Breaches Before and After ICT Adoption.

Period	Common Breaches	Characteristics	Professional Safeguards
Pre-ICT	File concealment, altered transcripts, gossip leaks	Slow, localized, traceable	Hierarchical clearance, paper security
Post-ICT	WhatsApp/email leaks, smartphone recordings, password tampering, viral circulation	Fast, viral, hard to trace	Weak enforcement, ICT misuse

Source: Authors' Analysis (2025)

Figure 1 provides a visual timeline of these changes, highlighting the evolution from localized, manual breaches in the pre-ICT era to fast, viral, and systemic breaches in the post-ICT era. This shift illustrates how confidentiality vulnerabilities have become more difficult to trace and control in the digital age.



Authors' Analysis (2025)

Figure 1. Timeline of confidentiality Breaches in Nigerian Universities.

3.4. Key Findings

1) Confidentiality demonstrates the strongest statistical correlation with effective administration, confirming it as the keystone professional practice.
2) ICT competence is both a positive enabler of efficiency and a key avenue for breaches.
3) The shift from paper to ICT has transformed breaches from localized and concealed to instantaneous, viral, and systemic.
4) Qualitative evidence confirms that weak sanctions, politicised appointments, and lack of professional regulation compound ICT-driven risks.

4. Discussion

This study set out to examine how confidentiality and ICT shape the effectiveness of university administration in Nigeria. The results reveal a striking paradox. Confidentiality remains the single most powerful predictor of effective governance (r =.972), yet it is simultaneously one of the weakest practiced domains in daily registry operations. This contradiction highlights a deeper institutional fragility: while the Registry is still regarded as the administrative core of the university, its professional ethos is being steadily eroded by weak enforcement, politicised leadership, and the disruptive effects of digital technology.

4.1. Confidentiality as the Keystone of Registry Professionalism

The evidence affirms that confidentiality is not a decorative virtue but the keystone of registry professionalism. Without it, other competencies—including ICT mastery, punctuality, or diligence cannot guarantee institutional trust. Confidentiality

is the condition that sustains credibility of certificates, integrity of council minutes, and confidence in admissions or staff records. The finding aligns with [9] insistence that the Registry is the "heartbeat" of the university and [1] description of registrars as custodians of secrets. When confidentiality collapses, the Registry risks losing its very identity as the guardian of governance.

4.2. ICT as a Double-Edged Sword

ICT competence also emerged as a significant positive predictor of administrative effectiveness (r =.801). On one hand, digital tools have expanded efficiency: electronic portals ease admissions, senate meetings can be virtual, and staff records are now searchable in seconds. On the other hand, the same tools have amplified confidentiality risks. In the paper-based era, breaches were slow, localized, and sometimes traceable—concealing files, altering transcripts, or leaking sensitive information to small groups. In contrast, today's breaches are instantaneous and viral. Unauthorized WhatsApp circulation of minutes, covert smartphone recordings of council meetings, and password tampering in e-transcript systems now define the everyday vulnerabilities of the Registry.

As depicted in Figure 1, breaches that once required deliberate actions and days or weeks to materialize now occur in seconds, often leaving universities with little chance to respond before information spreads widely. This finding underscores the argument that ICT adoption without enforceable safeguards magnifies confidentiality risks.

This dual character of ICT mirrors global experience. The University of Greenwich (UK) was fined £120,000 for GDPR breaches in 2018. A ransomware incident forced an institution to pay a substantial ransom [16], and another breach compromised academic records at scale [14] African universities are equally exposed: the University of Johannesburg mistakenly emailed confidential student data in 2022 [17], while Tshwane University of Technology was hit by ransomware in 2023. These cases show that ICT can strengthen governance only if it is embedded within a culture and system of confidentiality.

4.3. Institutional Theory: Why Practice Lags Behind Policy

Institutional Theory helps explain the contradiction observed in Nigerian universities. Institutions adopt ICT platforms, data protection policies, and compliance frameworks such as the Nigeria Data Protection Act (NDPA, 2023) under three forms of pressure:

1) *Coercive pressures* from government regulation.
2) *Normative pressures* from professional bodies like ANUPA and ARNU.
3) *Mimetic pressures* from imitating global ICT reforms.

However, as [13] argued, these adoptions often result in "decoupling", formal compliance structures exist on paper but are weakly enforced in practice. This explains why Nigerian universities can publicly claim NDPA compliance yet still suffer daily breaches via WhatsApp or cloud misuse. Confidentiality remains statistically central but practically neglected, because institutional legitimacy is projected through adoption, not through rigorous enforcement.

4.4. Weak Professional Safeguards and Cultural Drift

The findings also expose systemic weaknesses in professional regulation. Unlike professions such as accountancy (ICAN) or nursing (NMCN), registry practice in Nigeria lacks statutory regulation. ANUPA and ARNU remain advocacy associations without enforcement powers. As a result, breaches rarely attract consequences. Staff who leak council minutes are often transferred rather than disciplined. Politicisation of registrar appointments further dilutes professional accountability, replacing career administrators with politically aligned figures who may not prioritize confidentiality.

This lack of enforceable safeguards has produced a culture of impunity where breaches are normalized, especially among younger staff for whom digital sharing is instinctive. Without sanctions or strong professional identity, confidentiality erodes not just as a practice but as a value.

4.5. Broader Implications for Governance

The erosion of confidentiality in Nigerian universities carries three profound implications:

1) *Erosion of Trust* - Stakeholders lose faith in the integrity of certificates, transcripts, and governance decisions. Once trust is lost, even accurate records may be doubted.
2) *Exposure to Legal and Financial Sanctions* - Universities risk penalties under NDPA (2023), GDPR, and other global data protection laws, with consequences ranging from fines to reputational collapse.
3) *Professional Marginalisation of the Registry* - As breaches persist, the Registry's authority diminishes, ceding influence to ICT units or academics. This threatens its historic role as the administrative "engine room" of governance.

Confidentiality has shifted from being an ethical expectation to becoming a legal, financial, and reputational necessity. Failure to re-professionalise confidentiality will place Nigerian universities at risk of diminished governance credibility and weakened global competitiveness.

Table 3. Key Obligations under Nigeria Data Protection Act (NDPA, 2023).

Obligation	Description
Lawful Processing	Personal data must be collected and processed for legitimate purposes only
Data Minimisation	Only necessary data should be collected and retained
Breach Notification	Data breaches must be reported within 72 hours
Sanctions	Institutions face penalties and reputational risks for non-compliance

Source: Nigeria Data Protection Act (2023); Authors' Compilation (2025)

Table 4. Comparative Breaches in the Pre-Smartphone vs Post-Smartphone/Digital Era.

Dimension	Pre-Smartphone Era	Post-Smartphone / Digital Era
Mode	Physical alteration, gossip, photocopies	WhatsApp/email leaks, screenshots, recordings, cloud mismanagement
Speed	Slow (days-weeks)	Instant (seconds-minutes)
Scale	Localized, limited audience	Viral, potentially global
Detection	Late, sometimes years later	Immediate visibility but harder to contain
Impact	Small groups, localized disputes	Institution-wide damage, regulatory/legal penalties
Professional Culture	Deliberate, concealed breaches	Casual, normalized sharing via digital tools

Source: Authors' Analysis (2025)

The evidence presented in Table 4 further confirms that smartphones and digital platforms have accelerated the erosion of confidentiality. While breaches in the pre-smartphone era were deliberate, concealed, and limited in scope, the post-smartphone era has normalized instant sharing of sensitive information through screenshots, recordings, and social media forwarding. This cultural drift reflects not just technological change but also generational habits of disclosure, particularly among younger staff. Without clear ethical boundaries and enforceable sanctions, the Registry's professional identity risks being undermined by these casual digital practices.

5. Recommendations

Evidence from Nigerian, African, and global universities demonstrates that confidentiality is indispensable but increasingly vulnerable in the digital era. ICT has amplified risks, while generational shifts and weak professional enforcement have eroded registry professionalism. To restore credibility and align with global standards, the following recommendations are advanced:

5.1. Institutional Reforms Within Universities

1) *Embed Confidentiality in Organizational Culture:* Confidentiality should be institutionalized as a measurable professional competence rather than a symbolic tradition. Universities should require enforceable confidentiality oaths at induction and provide regular retraining to strengthen professional pride and accountability.
2) *Deploy Secure ICT Systems:* Confidentiality safeguards must be integrated into ICT infrastructure. Universities should adopt Management Information Systems (MIS) with multi-factor authentication, role-based access, and digital audit trails to prevent misuse and trace breaches.
3) *Strengthen Confidentiality Awareness for Gen Z Staff:* Targeted training should address the risks of screenshots, WhatsApp forwarding, and social media oversharing. Digital ethics must be emphasized alongside ICT competence to counter the culture of casual disclosure.
4) *Institutionalize Hybrid Work Readiness:* Post-pandemic realities require secure hybrid work policies. Confidentiality safeguards must extend to remote settings to protect sensitive information outside traditional office environments.
5) *Conduct Disruption Simulation Drills:* Confidentiality breaches should be treated as institutional emergencies. Simulation exercises—similar to fire drills—can test preparedness and improve response capacity.

6) *Promote Foresight and Digital Resilience:* Recognizing disruption as the "new normal," universities must embed resilience planning to safeguard confidentiality during crises, from pandemics to cyberattacks.

5.2. Professional Associations (ANUPA and ARNU)

1) *Transform into Regulatory Bodies:* ANUPA and ARNU should evolve from advocacy platforms into statutory regulatory bodies, modelled after ICAN (accountants) or NMCN (nurses), with authority to accredit training, certify competence, and discipline members.
2) *Introduce Confidentiality Certification and CPD:* Confidentiality should be formally certified as a core competence. Continuous Professional Development (CPD) on ICT ethics, NDPA compliance, and information governance should be mandatory for career progression.
3) *Enforce Sanctions for Breaches:* Confidentiality violations must attract enforceable sanctions, ranging from suspension to deregistration. This would address the prevailing culture of impunity and elevate professional accountability.

5.3. National Policy and Legal Frameworks

1) *Establish NDPA-Aligned Compliance Units:* Each university should create a Confidentiality and Data Protection Unit responsible for annual audits, staff training, and breach reporting within the NDPA's 72-hour requirement.
2) *Recognize Registry Administration as a Profession:* The Federal Ministry of Education and the National Universities Commission (NUC) should formally recognize registry administration as a profession with statutory protections, career pathways, and enforceable codes of practice.
3) *Integrate with Global Standards:* Nigeria should benchmark confidentiality enforcement against international frameworks such as GDPR (EU), FERPA (USA), and POPIA (South Africa). Alignment with global standards will strengthen institutional credibility and graduate mobility.

Confidentiality is the keystone of registry professionalism, while ICT serves as both enabler and risk. Embedding confidentiality in institutional culture, enforcing it through professional bodies, and legislating it at the national level are essential. Without such reforms, trust will continue to erode; with them, the Registry can reclaim its role as the core of university governance.

6. Conclusion

This study demonstrates that confidentiality is the keystone of effective university administration in Nigeria. The evidence is unambiguous. Confidentiality shows the strongest statistical link to governance effectiveness (r =.972); however, it remains the weakest practiced competency in daily registry work. ICT, while vital for efficiency, has amplified opportunities for breaches, transforming once-localized lapses into viral disclosures that undermine trust and expose universities to legal and reputational risks.

The contribution of this research lies in clarifying a central contradiction in registry practice: universities adopt ICT platforms and compliance frameworks such as the Nigeria Data Protection Act (NDPA, 2023) to project legitimacy, yet confidentiality is not consistently enforced in practice. By applying Institutional Theory, the study interprets this gap as a form of "decoupling" between formal policy and operational reality.

For Nigerian universities, the implications are clear. Confidentiality must be redefined as a measurable professional competence, safeguarded through enforceable policies, ICT-based protections, and statutory regulation of registry practice. Without such reforms, the Registry risks sliding into irrelevance; with them, it can reclaim its role as the trusted custodian of governance in the digital age.

Ultimately, confidentiality is not merely an ethical expectation but the foundation of institutional credibility. Its preservation is essential for restoring trust, strengthening governance, and maintaining the Registry's role as the primary safeguard of university administration.

Abbreviations

ANUPA	Association of Nigerian University Professional Administrators
ARNU	Association of Registrars of Nigerian Universities
FERPA	Family Educational Rights and Privacy Act
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
NDPA	Nigeria Data Protection Act
POPIA	Protection of Personal Information Act

Author Contributions

Edho Okugbe Genesis: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Validation, Visualization, Writing – original draft, Writing – review & editing

Akpotu Nelson Ejiro: Methodology, Supervision, Validation, Writing – review & editing

Asiyai Romina Ifeoma: Methodology, Supervision, Validation, Writing – review & editing

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Onyemakonor, A. A. (2007). Keynote address by the Registrar, Delta State University, 1st in-house training programme organised by ANUPA DELSU. Unpublished work.

[2] Iniama, E. B. (2015). Covering meetings: Standard minutes writing. Paper presented at the Association of Nigerian University Professional Administrators Conference.

[3] Asukwo, I. (2021). A practical guide to administrative and executive duties in Nigerian universities. Bloann Educational Publishers.

[4] Edho, O. G., & Ogini, O. (2018). Towards a "paperless" higher education system in Nigeria. Journal of Education, Society and Behavioural Science, 24(2), 1-15. https://doi.org/10.9734/JESBS/2018/19913

[5] Zaman, U., Nawaz, S., & Nadeem, R. D. (2020). Navigating innovation success through projects: Role of CEO transformational leadership, project management best practices, and project management technology quotient. Journal of Open Innovation: Technology, Market, and Complexity, 6(4), 168. https://doi.org/10.3390/joitmc6040168

[6] Afebende, G., & Orim, F. S. (2018). Records management practices at the registry of four selected universities in South-South region of Nigeria. Lagos Journal of Library & Information Science, 7(1), 1-15.

[7] Ajike, C. F., Alegbeleye, G. O., Madukoman, E., & Babalola, Y. T. (2021). Self-efficacy of records personnel and student records management practices in South-West Nigerian university registries. International Journal of Academic Library and Information Science, 9(4), 172-179. https://doi.org/10.14662/IJALIS2021.145

[8] Edho, O. G. (2025). Registry personnel best practices and effective university administration in South-South Nigeria (Unpublished doctoral dissertation).

[9] Okebukola, P. A. (2000). The registry as the heart of the university system: Making it beat efficiently. Second Registry Lecture, Elizade University, Ilara-Mokin.

[10] Nkedishu, A., & Okonta, B. (2024). Artificial intelligence and ethics in African higher education governance. Journal of African Studies and Research, 17(2), 143-160.

[11] Illidge, M. (2024, Feb). Tshwane University of Technology suffers ransomware attack — thousands of records stolen. MyBroadband. Retrieved from https://mybroadband.co.za/news/security/524680-tshwane-university-of-technology-suffers-ransomware-attack-thousands-of-records-stolen.html

[12] News24. (2024, February 12). Major data breach at Tshwane University of Technology leads to suspension of deputy vice-chancellor. News24. Retrieved from https://www.satorinews.com/articles/2024-02-12/major-data-breach-at-tshwane-university-of-technology-leads-to-suspension-of-deputy-vc-181814

[13] Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. American Journal of Sociology, 83(2), 340-363. https://doi.org/10.1086/226550

[14] Australian National University. (2019). Public incident report on the 2018 data breach. https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf

[15] Bloomberg. (2020, June 29). The University of California pays $1 million ransom following cyber-attack. Forbes. Retrieved from https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/

[16] University of California, San Francisco. (2020, June 26). Update on IT security incident at UCSF. https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf

[17] Business Report / IOL. (2022, September 29). Cyber security: Universities under fire (University of Johannesburg incident; University of Mpumalanga attack). https://iol.co.za/

[18] Ufiofio, R. U. (2024, August 24). 2024 Registry Lecture: Welcome address by the University Registrar. Abraka.

[19] Rama, P. (2025). Cybersecurity awareness among accounting students at a South African public university. South African Journal of Information Management, 27(1). https://scielo.org.za/pdf/sajim/v27n1/16.pdf